Recomendações de Segurança CAIS/RNP:
Modelo para equipamentos de infra-estrutura

Ivo de Carvalho Peixinho

Março de 2006

O presente documento apresenta as recomendações de segurança do Centro de Atendimento a Incidentes de Segurança da RNP, a serem consideradas no processo de configuração dos equipamentos de infra-estrutura da RedeComep. As mesmas referem-se apenas à proteção dos equipamentos de rede, não especificando nenhum tipo de equipamento de segurança adicional para o projeto.

RNP/REF/0211

Sumário

1.
Introdução

Este documento apresenta uma série de recomendações de configuração para equipamentos de infra-estrutura da RedeComep, visando aumentar a segurança desta rede. Estas recomendações, juntas, constituem um **modelo de segurança**, que deve ser aplicado nos equipamentos de rede dos consórcios participantes. Este modelo deverá ser traduzido em regras e parâmetros de configuração específicos para cada modelo de equipamento.

Para cada recomendação serão apresentadas uma descrição resumida, além de comentários e quaisquer outras observações relevantes.

2.
Recomendações

1. Desabilitar serviços e protocolos desnecessários

Muitos equipamentos de rede dispõem de serviços diversos, que não estão relacionados diretamente ao funcionamento do equipamento, ou só se aplicam em casos mais específicos. Como exemplos podemos citar os servidores *http* internos de configuração, servidores DHCP/bootp de fornecimento de endereços IP, serviços TCP/UDP simples (echo, discharge, time, etc), serviço finger para obter informações de usuários, protocolos proprietários de fabricantes como CDP (Cisco Discovery Protocol), serviços de transferência de arquivo sem senha (tftp), serviços de identificação de usuários (identd), proxy-arp e muitos outros. A recomendação é sempre desabilitar estes serviços e só habilitá-los se realmente forem usados. Caso estes serviços necessitem serem usados, definir regras de acesso ao serviço para permitir acesso apenas a clientes autorizados.

2. Desabilitar *source-route*, caso não seja desabilitado na configuração padrão

O recurso *source-route* é um recurso antigo presente na família TCP/IP, que permite que um pacote seja enviado e seja definido previamente o caminho do pacote até o destino. Este recurso, caso habilitado, pode causar sérios problemas de segurança, visto que um atacante pode forjar um pacote e entregá-lo por um caminho específico. Nos equipamentos mais modernos, este recurso costuma vir desabilitado na configuração padrão. A recomendação é desabilitar este recurso, independente do equipamento.

3. Configurar recurso *anti-spoofing*, caso exista

O recurso *anti-spoofing* habilita um roteador ou um *switch* a descartar pacotes que não estejam de acordo com as tabelas de roteamento existentes no mesmo. Este tipo de recurso evita que usuários internos da rede enviem pacotes com endereços externos e vice-versa, o que caracterizaria uma atividade de *spoofing* (falsificação) de pacotes.

4. Configurar filtros para impedir entrada de pacotes com endereços de origem pertencentes a redes internas e a saída de pacotes com endereços de origem pertencentes a redes externas (filtros *egress* e *ingress*)

Estes filtros seguem o mesmo princípio do recurso *anti-spoofing*, e devem ser aplicados no equipamento, especialmente se o mesmo não dispor de um recurso *anti-spoofing* específico. Maiores informações sobre *anti-spoofing*, *ingress* e *egress filters* podem ser obtidas na RFC 2827.

5. Configurar senhas fortes e protegidas por funções *hash* para todas as contas

Em alguns equipamentos de rede, as senhas dos usuários locais são armazenadas na forma literal (texto limpo), sendo inclusive apresentadas na listagem da configuração do equipamento. Todas as senhas devem ser armazenadas utilizando algum recurso que dificulte a descoberta da senha, mesmo que os dados de configuração sejam obtidos por terceiros. A forma mais comum de atingir este objetivo é através da cifragem das senhas utilizando uma função *hash one-way* (ex: MD5).

6. Configurar contas para usuários. Evitar acessar o sistema diretamente com a senha de administrador

Especialmente quando existem muitos administradores de um mesmo equipamento, é importante que cada um tenha uma conta de usuário, e a utilize para entrar no equipamento. Desta forma os registros de acesso terão a informação sobre quem realizou determinada tarefa de administração. Esta prática ainda dificulta acessos indevidos, pois um atacante necessitará obter a senha pessoal de um dos administradores e a senha de administrador propriamente dita.

7. Configurar ao menos uma conta local no equipamento

É comum a utilização de serviços de autenticação remota, como TACACS e RADIUS para autenticação de usuários nos equipamentos, de modo que não seja necessário criar contas para todos os administradores em cada equipamento. Neste caso, é importante existir pelo menos uma conta local, de modo que seja possível entrar no equipamento, mesmo que o servidor de autenticação ou a rede que interliga os dois esteja indisponível.

8. Configurar corretamente o *timezone* e o horário do equipamento, incluindo horário de verão e sincronização de tempo

Manter o horário correto nos equipamentos de rede é de vital importância, visto que todos os registros de *log* contem o horário em que o evento ocorreu, incluindo o *timezone*. É muito importante utilizar uma fonte de tempo confiável e sincronizar o relógio de todos os equipamentos a partir desta fonte de tempo. Recomenda-se o uso do protocolo NTP para este fim, pois se trata de um protocolo padrão e bastante utilizado na Internet.

9. Desabilitar *broadcasts* direcionados para prevenir ataques smurf

Broadcasts direcionados são difusões para uma rede inteira, onde a origem do pacote se encontra fora da rede em questão. Apesar de ser permitido de acordo com o padrão TCP/IP, este tipo de atividade pode permitir que um atacante gere uma série de respostas para um pacote que veio de fora da rede. A recomendação é que somente máquinas da própria rede possam enviar *broadcasts* na rede. Alguns fabricantes possuem comandos específicos para tal fim.

10. Manter informações de *netflow* e, se possível, exportar para um servidor de log

O recurso *netflow* permite armazenar informações sobre conexões efetuadas e quantos *bytes* e pacotes foram transmitidos naquela conexão. Esta informação é muito útil na detecção de tráfego anômalo na rede. Apesar do volume de informação ser grande em um *backbone*, é importante armazenar esta informação, mesmo que seja por um período de tempo reduzido. A maioria dos equipamentos permite ainda que se exporte esta informação para um servidor à parte, onde a informação pode ser analisada. O *netflow* hoje é uma das formas mais comuns de detectar ataques DDoS e atividades de *worm*.

11. Criar rotas "nulas" e filtros de acesso para redes falsas e inativas

Muitos programas maliciosos “sorteiam” endereços IP em busca de novas máquinas para infectar. Muitas vezes estes programas acessam endereços que não estão em uso na Internet. Bloquear e registrar o acesso a estes endereços pode diminuir o tráfego destes programas, além de proteger a rede. Dentre os endereços que não estão em uso, temos os reservados pelo IANA e os ainda não alocados para nenhum país. Uma listagem destes endereços pode ser encontrada no anexo. Uma questão importante a considerar é que os endereços não alocados são alterados de tempos em tempos, então estes bloqueios têm que ser revistos periodicamente. O endereço a seguir contem a lista atual de endereços inválidos na Internet (conhecidos como *bogons)*: *http://www.cymru.com/Documents/bogon-dd.html*

12. **Limitar e controlar acesso SNMP**

O protocolo SNMP, muito utilizado para gerência de redes e monitoramento, é um protocolo bastante frágil no que tange à segurança, então seu uso deve ser bastante restrito. Caso ele não seja necessário, a recomendação é desabilitar completamente o protocolo SNMP. Caso ele precise ser utilizado, recomenda-se remover quaisquer comunidade*s* publicas, criar comunidades com nomes complexos (o nome da comunidade é a senha para acesso à mesma) e somente read-only. Adicionalmente deve-se considerar o uso de filtros de pacotes para restringir o acesso ou até a utilização de uma VLAN de gerência (veja abaixo) apenas para acesso SNMP. Deve-se ainda considerar o uso do SNMPv3 se possível (esta versão inclui criptografia e autenticação de usuários).

13. Definir uma VLAN de gerência

A maior parte dos equipamentos de infra-estrutura atuais permite a criação de redes físicas virtuais, de modo que seja possível a separação de tráfego no nível físico. Recomenda-se criar uma VLAN de gerenciamento que seja propagada entre todos os dispositivos e que os equipamentos tenham endereços falsos nesta VLAN, de modo que exista um acesso privilegiado apenas por esta VLAN. As estações de gerência e de administração também devem participar desta VLAN. Recomenda-se não utilizar a VLAN 1 para este fim, visto que é a VLAN *default* de qualquer equipamento recém-instalado.

14. Desabilitar portas fora de uso

Recomenda-se desabilitar todas as portas de acesso e de tronco que não estejam sendo usadas, além de colocá-las em uma VLAN que não esteja sendo utlizada. Nenhuma porta de nenhum equipamento deve ser alocada para a VLAN *default* (VLAN 1).

15. Manter registro de todo tráfego bloqueado

Todos os pacotes bloqueados pelos equipamentos de rede devem ter um registro de bloqueio, contendo a data e hora, endereços IP, portas e parâmetros TCP/IP envolvidos. Esta informação será útil para descobrir a razão do tráfego ter sido bloqueado e a identidade dos responsáveis pelo tráfego.

16. Manter registro de todos os eventos ocorridos nos equipamentos de rede e exportar os registros de log do sistema para um servidor a parte (loghost)

Todos os equipamentos devem ser configurados para registrar os eventos relevantes em um *buffer* ou arquivo de log. Preferencialmente, deve-se alocar um servidor responsável por receber e armazenar este log no formato *syslog*, com um sistema de salvaguarda (*backup*) apropriado.

17. Configurar um *banner* adequado nos equipamentos

Caso o protocolo permita, o sistema deve apresentar um aviso a qualquer usuário que tente se conectar ao equipamento. Este aviso deve deixar claro que acessos não autorizados não serão permitidos e que todos os acessos e tentativas serão registrados.

18. Limitar o acesso remoto ao equipamento

Utilizar a VLAN de gerenciamento e/ou outros recursos como listas de acesso para permitir o acesso remoto apenas a endereços IP confiáveis. Este acesso deve ainda possuir um esquema de *timeout*, de modo que sessões inativas sejam automaticamente desconectadas.

19. Desabilitar acessos não criptografados aos equipamentos

Serviços como *telnet* e *http* devem ser desabilitados e substituídos por versões criptografadas e conseqüentemente mais seguras. Utilizar *ssh* e *https* respectivamente em substituição a estes últimos. Alterar a porta padrão destes serviços de modo que seja mais difícil um ataque de força bruta ou uma exploração de vulnerabilidades.

20. Habilitar autenticação nos protocolos de roteamento dinâmicos

Protocolos como BGP e OSPF hoje utilizam formas de autenticação, de modo que terceiros não sejam capazes de trocar rotas com os equipamentos legítimos da rede. Deve-se ainda considerar a criação de listas de distribuição, de modo que haja um controle dos prefixos de rede recebidos e enviados pelos protocolos de roteamento.

21. Realizar backups periódicos das configurações dos roteadores e switches, e analisar as mudanças entre elas

Antes de qualquer alteração na configuração de qualquer equipamento, deve ser feita uma cópia de segurança da configuração, indicando inclusive a data da alteração e o responsável. Deve-se ainda automatizar ou realizar de forma manual um processo de comparação da configuração atual com a última configuração armazenada, de modo a detectar mudanças não autorizadas na configuração do equipamento.

22. Aplicar todas as correções de segurança disponibilizadas pelos fabricantes

Em se tratando de equipamentos de rede, a atualização do sistema operacional e *firmware* do equipamento, não é tão comum quando a atualização de sistemas operacionais de *desktop*, visto que estas plataformas, em geral, são mais robustas e as atualizações de versão podem trazer novos recursos que causem instabilidade no equipamento. Apesar disto, é importante que, caso exista uma correção **de segurança** para o equipamento, esta deve ser aplicada no menor intervalo de tempo possível.

23. Fixar os endereços físicos (MAC) de roteadores e *switches* nas tabelas dos equipamentos

O protocolo ARP, presente no nível 2 da família TCP/IP, identifica interfaces de equipamentos pelo seu MAC address, que consiste em um conjunto de 6 bytes que normalmente é fisicamente gravado na interface de rede. Apesar desta identificação física, é um processo relativamente simples alterar este endereço e, conseqüentemente, enviar quadros com o endereço físico falsificado (forjado). Uma forma simples de dificultar este processo, é fixar a associação entre os endereços IP e os endereços MAC dos equipamentos sensíveis nas tabelas internas dos *switches* e roteadores. Desta forma o equipamento sabe previamente o endereço físico correspondente aos endereços IP dos equipamentos e vice-versa.

24. Utilizar autenticação 802.1x em equipamentos críticos

O protocolo 802.1x permite que componentes da rede sejam autenticados antes do acesso deles à rede seja liberado. Este recurso permite aos administradores dispor de um controle maior sobre conexões não autorizadas e clandestinas aos equipamentos de rede, além de facilitar o bloqueio de equipamentos comprometidos.

25. Promover separação de tráfego através de VLAN's entre as instituições parceiras e o backbone do consórcio

Apesar de adicionar *overhead*, a separação de tráfego no nível 3 (*roteamento*) entre cada instituição e o *backbone* do consórcio garante que o tráfego interno à instituição não circule desnecessáriamente fora da mesma, incluindo *broadcasts*. Esta condição é desejável tanto por questões de segurança como para se evitar a transmissão desnecessária de informação pelo *backbone*. A forma que esta separação será realizada vai depender de acordo com a topologia de cada consórcio, porém ela deve contemplar, no mínimo, que haja uma separação nível 3 na fronteira da instituição com o *backbone*.

3.

Anexo 1 – Lista de Bogons em 05 JAN 2006 (v3.0) – Versão agregada

0.0.0.0 254.0.0.0
2.0.0.0 255.0.0.0
5.0.0.0 255.0.0.0
7.0.0.0 255.0.0.0
10.0.0.0 255.0.0.0
23.0.0.0 255.0.0.0
27.0.0.0 255.0.0.0
31.0.0.0 255.0.0.0
36.0.0.0 254.0.0.0
39.0.0.0 255.0.0.0
42.0.0.0 255.0.0.0

49.0.0.0 255.0.0.0
50.0.0.0 255.0.0.0
77.0.0.0 255.0.0.0
78.0.0.0 254.0.0.0
92.0.0.0 252.0.0.0
96.0.0.0 240.0.0.0
112.0.0.0 248.0.0.0
120.0.0.0 255.0.0.0
127.0.0.0 255.0.0.0
169.254.0.0 255.255.0.0
172.16.0.0 255.240.0.0
173.0.0.0 255.0.0.0
174.0.0.0 254.0.0.0
176.0.0.0 248.0.0.0
184.0.0.0 252.0.0.0
192.0.2.0 255.255.255.0
192.168.0.0 255.255.0.0
197.0.0.0 255.0.0.0
198.18.0.0 255.254.0.0
223.0.0.0 255.0.0.0
224.0.0.0 224.0.0.0

4. Anexo 2 – Endereços reservados no IANA (RFC 1918)

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

5. Referências

Secure IOS Template Version 4.2 05 JAN 2006
By Rob Thomas, robt at cymru.com
http://www.cymru.com/Documents/secure-ios-template.html

Protecting your IP network infrastructure
Nicolas FISCHBACH
Sébastien LACOSTE-SERIS

RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
http://www.faqs.org/rfcs/rfc2827.html

RFC 1918 - Address Allocation for Private Internets
http://www.faqs.org/rfcs/rfc1918.html