

O Uso de Firewalls na Segurança de Redes

Thiago Silvino

25/11/2013

Fundação Bradesco Campinas

Palestrante

Thiago Silvino www.silvino.net

Especialista em Segurança de Redes – AT&T
www.att.com

Atua na área de redes de computadores desde
2002

Objetivo da Palestra

Temas abordados:

- 1 – Conceitos de redes de computadores
- 2 – Equipamentos de rede
- 3 – Funcionamento de firewalls
- 4 – Packet filtering e stateful inspection
- 5 – Antispoofing
- 6 – NAT e VPNs

Redes de Computadores

Interconexão entre equipamentos

Transmissor, meio de transmissão e receptor

Envio e recebimento de informações

Compartilhamento de recursos (discos, arquivos, conexões)

Modelos de rede TCP/IP e OSI

| Equipamento | Unidade | TCP/IP | OSI |
|-------------------------------|------------------|---------------|-----------------|
| Firewall, proxy, loadbalancer | Dados | 5. Aplicação | 7. Aplicação |
| | | | 6. Apresentação |
| | | | 5. Sessão |
| | Segmento | 4. Transporte | 4. Transporte |
| Roteadores | Pacote/datagrama | 3. Rede | 3. Rede |
| Switches e bridges | Quadro | 2. Enlaçe | 2. Enlaçe |
| Hub, Cabos e conectores | Bit | 1. Física | 1. Física |

Equipamentos de rede

Para interconectar os computadores podemos usar vários equipamentos

1 – Switches e access-points: usados para fazer a conexão física das placas de rede

2 – Roteadores: utilizados para encaminhar pacotes entre várias redes

3 – Firewalls: usados para interligar as redes de forma segura

Endereçamento de rede

Exemplo de endereçamento de uma placa de rede sem fio

| Network Connection Details: | |
|-----------------------------|--------------------------------------|
| Property | Value |
| Connection-specific... | |
| Description | Intel(R) Centrino(R) Advanced-N 6205 |
| Physical Address | 8C-70-5A-1D-02-34 |
| DHCP Enabled | Yes |
| IPv4 Address | 192.168.0.14 |
| IPv4 Subnet Mask | 255.255.255.0 |

Topologia de rede

Firewall

- Usando um firewall podemos criar regras de acesso para as suas redes
- Cada regra define os endereços de origem (quem inicia a comunicação), endereços de destino (qual endereço será acessado), protocolos e ação (ACCEPT, DROP, REJECT)
- O firewall olha a tabela de regras de cima para baixo e aplica a primeira que se aplicar a conexão

Tipos de firewall

1 – Filtro de pacotes

Nesse tipo de firewall devemos definir regras em todas as interfaces de rede do firewall. Devemos criar regras específicas para garantir o retorno dos pacotes.

2 – Stateful inspection

Um firewall com a tecnologia stateful inspection usa uma tabela de conexões para garantir o retorno dos pacotes. A empresa Check Point patenteou essa tecnologia e a incluiu no seu produto FireWall-1 em 1994 .

Ferramentas: Firewall CheckPoint

Principais programas do SmartConsole:

- SmartDashboard: tabela de regras de segurança, NAT, Application & URL Filtering, Data Loss Prevention, IPSec VPN e QoS.
- SmartView Tracker: Visualização de Logs
- SmartMonitor: Monitoração de status dos firewalls
- SmartUpdate: Upgrade de software e manutenção de licenças e contratos

Exemplo: SmartDashboard

| No. | Hits | Name | Source | Destination | VPN | Service | Action | Track | Install On | Time | Comment |
|--|--|----------------------|------------------------------------|--|-------------|-----------------------------------|-------------|-------|----------------|------|--|
| Limit Access to Gateways Rule (Rule 1) | | | | | | | | | | | |
| 1 | <div><div></div><div></div><div></div><div></div></div> 0 | Stealth | Corporate-internal-net | GW-group | Any Traffic | Any | drop | Alert | Policy Targets | Any | Stealth rule - prevent the VPN firew host from being scanned or attacked |
| VPN Access Rules (Rules 2-5) | | | | | | | | | | | |
| Rules for Specific Sites (Rules 6-8) | | | | | | | | | | | |
| 6 | <div><div></div><div></div><div></div><div></div></div> 21K | Outbound HTTP | Remote-2-internal | Any | Any Traffic | http | ClientAuth | Log | Remote-2-gw | Any | Audit all outbound user HTTP conn from remote-2-internal using UserAuthority |
| 7 | <div><div></div><div></div><div></div><div></div></div> 47K | Critical subnet | Corporate-internal-net | Corporate-finance-net Corporate-hr-net Corporate-rnd-net | Any Traffic | Any | accept | Log | Corporate-gw | Any | Log traffic to critical subnets - only enforce this rule on the Corporate-g |
| 8 | <div><div></div><div></div><div></div><div></div></div> 3K | Tech support | Tech-Support | Remote-1-web-server | Any Traffic | http | accept | Alert | Remote-1-gw | Any | Allow technical support access to v server - only enforce this rule on Remote-1-gw |
| Identity Based Access (Rules 9-12) | | | | | | | | | | | |
| Common Rules - All Sites (Rules 13-19) | | | | | | | | | | | |
| 13 | <div><div></div><div></div><div></div><div></div></div> 4M | Terminal server | Corporate-internal-terminal-server | Any | Any Traffic | Any | SessionAuth | Log | Corporate-gw | Any | Audit all traffic from terminal server using UserAuthority |
| 14 | <div><div></div><div></div><div></div><div></div></div> 2K | DNS server | Any | Corporate-dns-ext | Any Traffic | UDP domain-udp | accept | None | Policy Targets | Any | Allow domain name queries to exte DNS server |
| 15 | <div><div></div><div></div><div></div><div></div></div> 672K | SOAP | Any | Corporate-IVA-proxy-server | Any Traffic | http->SOAP-requests | accept | Log | Policy Targets | Any | Allow only selected SOAP methods block all others |
| 16 | <div><div></div><div></div><div></div><div></div></div> 0 | Mail and Web servers | Any | Corporate-dmz-net | Any Traffic | TCP http TCP https TCP smtp | accept | Log | Policy Targets | Any | Allow incoming connections to the n and web servers |
| 17 | <div><div></div><div></div><div></div><div></div></div> 663K | SMTP | Corporate-mail-server | Internal-net-group | Any Traffic | smtp | accept | Log | Policy Targets | Any | Allow outgoing SMTP connections, t don't allow the mail server to initiate connections to the internal networks case it is compromised |
| 18 | <div><div></div><div></div><div></div><div></div></div> 66K | DMZ and Internet | Internal-net-group | Any | Any Traffic | Any | accept | Log | Policy Targets | Any | User access to DMZ servers and Int |
| 19 | <div><div></div><div></div><div></div><div></div></div> 3M | Clean up rule | Any | Any | Any Traffic | Any | drop | Log | Policy Targets | Any | Clean up rule - block all other connections |

Exemplo: SmartView Tracker

Network & Endpoint Q...

Active

Management

Network & Endpoint Q...

Predefined

All Records

Network Security

Firewall Blade

IPS Blade

Application

HTTPS Inspe

Anti-Bot & A

Identity Awa

Anti-Spam &

Mobile Acce

Data Loss Pr

IPSEC VPN B

Advanced N

Traditional A

Voice over IP

More

Firewall-1 G

UTM-1 Edge

Monitoring

Endpoint Secur

All Endpoint

Compliance

Firewall Ever

Blocked Pro

Antivirus

No.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

11/29

Alaska_mem...

California_GW

California_GW

California_GW

California_GW

California_GW

California_GW

California_GW

Alaska_RND_...

Alaska_cluster

Alaska_cluster

Alaska_cluster

Alaska_cluster

Alaska_cluster

Alaska_cluster

Alaska_mem...

Alaska_cluster

Primary_Man...

Alaska_cluster

Alaska_Finan...

Alaska_RND_...

Alaska_RND_...

Alaska_RND_...

Alaska_cluster

Alaska_cluster

Alaska_cluster

Alaska_cluster

Alaska_cluster

Alaska_cluster

11:29

15:00:41

15:06:33

15:41:29

16:43:13

17:43:28

18:35:11

18:35:14

18:39:42

8:10:20

8:11:22

8:11:30

8:12:29

8:14:36

8:14:38

11:14:26

1:00:1

2:14:36

2:19:21

10:9:29

10:9:30

10:9:31

16:35:14

16:35:19

22:54:13

22:54:13

22:54:13

22:54:13

22:54:13

SMTP

SMTP

SMTP

SMTP

SIP

SMTP

TCP

TCP

HTTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

HTTP

Microsoft-DS

8080

8080

8080

HTTP

HTTP

HTTP

HTTP

HTTP

HTTP

California.LAN.ha...

California.LAN.ha...

California.LAN.ha...

voip

California.LAN.jac...

35.12.10.129

10.111.254.11

robot.fps.domain...

robot.fps.domain...

robot.fps.domain...

robot.fps.domain...

robot.fps.domain...

robot.fps.domain...

robot.fps.domain...

resolved.hosts.com

Alaska.IT.Bentli

10.111.254.31

10.111.254.31

10.111.254.31

scriptkids.inc

scriptkids.inc

California.LAN.jac...

California.LAN.jac...

California.LAN.ha...

rule 4

rule 4

rule 4

rule 4

rule 3

rule 10

rule 4

rule 12

rule 15

rule 15

rule 15

rule 15

rule 15

rule 15

rule 15

rule 15

rule 15

rule 15

rule 11

rule 12

rule 12

rule 14

rule 14

rule 14

rule 14

rule 14

rule 14

4805

4805

2972

10008

2693

80

1208

34501

34555

34497

34533

35421

34533

35421

32818

32818

33822

33822

1208

1208

1208

1208

1208

1208

1208

1208

1208

user1

user1

user1

user2

user2

user2

user2

user2

user3

user3

user3

user3

user3

user3

user3

user4

user4

user4

user5

user6

user4

user4

user4

user4

MR. TES

MR. TES

MR. TES

Exemplo: SmartView Tracker accept

Record Details

PreviousNextCopy Details

Security Gateway/Management

Log Info

| | |
|---------|-----------------------------|
| Product | Security Gateway/Management |
| Date | 1Nov2008 |
| Time | 15:06:33 |
| Number | 3 |
| Type | Log |
| Origin | California_GW (192.7.100.2) |

Rule

| | |
|---------------------|------------|
| Action | Accept |
| Rule | 4 |
| Current Rule Number | 4-Standard |
| Rule Name | rule 4 |
| User | user1 |

More

Information

agent: mail dequeuer; number of recipients: 1
orig_from: <denkiy@abc-corp.biz>
to: <denkiy@abc-corp.biz>

Traffic

| | |
|-------------|--|
| Source | California.LAN.hamilton (172.16.2.120) |
| Destination | durden.abc-corp.biz |
| Service | smtp (25) |
| Protocol | tcp |
| Interface | daemon |
| Source Port | 4805 |

Policy

| | |
|-------------------|--------------------------|
| Policy Name | Standard |
| Policy Date | Sun Oct 27 08:40:46 2002 |
| Policy Management | California_GW |

Multi-product

Record Details

PreviousNextCopy Details

Security Gateway/Management

Log Info

| | |
|---------|-----------------------------|
| Product | Security Gateway/Management |
| Date | 15Jan2009 |
| Time | 22:59:34 |
| Number | 27 |
| Type | Log |
| Origin | California_GW (192.7.100.2) |

Rule

| | |
|---------------------|------------|
| Action | Encrypt |
| Rule | 2 |
| Current Rule Number | 2-Standard |
| Rule Name | rule 2 |
| User | ... |

More

Destination Key ID

0x63a1a1e2

Encryption Scheme

ESP: 3DES + MD5

Encryption Methods

Delaware_cluster (191.18.34.100)

VPN Peer Gateway

...

Information

Traffic

| | |
|-------------|--|
| Source | California.LAN.hamilton (172.16.2.120) |
| Destination | Alaska.LAN.Chincilla (10.100.254.111) |
| Service | rbsession (139) |
| Protocol | tcp |
| Interface | qler7 |
| Source Port | 4780 |

Policy

| | |
|-------------------|-----|
| Policy Name | ... |
| Policy Date | ... |
| Policy Management | ... |

Exemplo: SmartView Tracker drop

Record Details

PreviousNextCopy Details

Security Gateway/Management

Log Info

| | |
|---------|-----------------------------|
| Product | Security Gateway/Management |
| Date | 1Nov2008 |
| Time | 18:35:14 |
| Number | 8 |
| Type | Log |
| Origin | California_GW (192.7.100.2) |

Rule

| | |
|---------------------|------------|
| Action | Drop |
| Rule | 4 |
| Current Rule Number | 4-Standard |
| Rule Name | rule 4 |
| User | user2 |

More

Traffic

| | |
|-------------|---------------|
| Source | 35.12.10.129 |
| Destination | California_GW |
| Service | 1039 |
| Protocol | TCP tcp |
| Interface | E190x1 |
| Source Port | 80 |

Policy

| | |
|-------------------|-----|
| Policy Name | ... |
| Policy Date | ... |
| Policy Management | ... |

Information

Record Details

PreviousNextCopy Details

Security Gateway/Management

Log Info

| | |
|---------|------------------------------|
| Product | Security Gateway/Management |
| Date | 2Nov2008 |
| Time | 8:10:20 |
| Number | 10 |
| Type | Log |
| Origin | Alaska_cluster (207.33.42.4) |

Rule

| | |
|---------------------|-------------|
| Action | Reject |
| Rule | 15 |
| Current Rule Number | 15-Standard |
| Rule Name | rule 15 |
| User | user3 |

More

Traffic

| | |
|-------------|--|
| Source | robot.https.domain.com |
| Destination | Alaska_DMZ_internal_web (172.31.254.2) |
| Service | ftp (21) |
| Protocol | TCP tcp |
| Interface | E190x1 |
| Source Port | 34501 |

Policy

| | |
|-------------------|--------------------------|
| Policy Name | Standard |
| Policy Date | Mon Oct 21 07:04:09 2002 |
| Policy Management | Primary_Management |

Information

| | |
|-------------|---|
| XlateDst | 207.33.42.2 |
| Information | message info: Port command ended without a new line |

Exemplo: SmartView Tracker

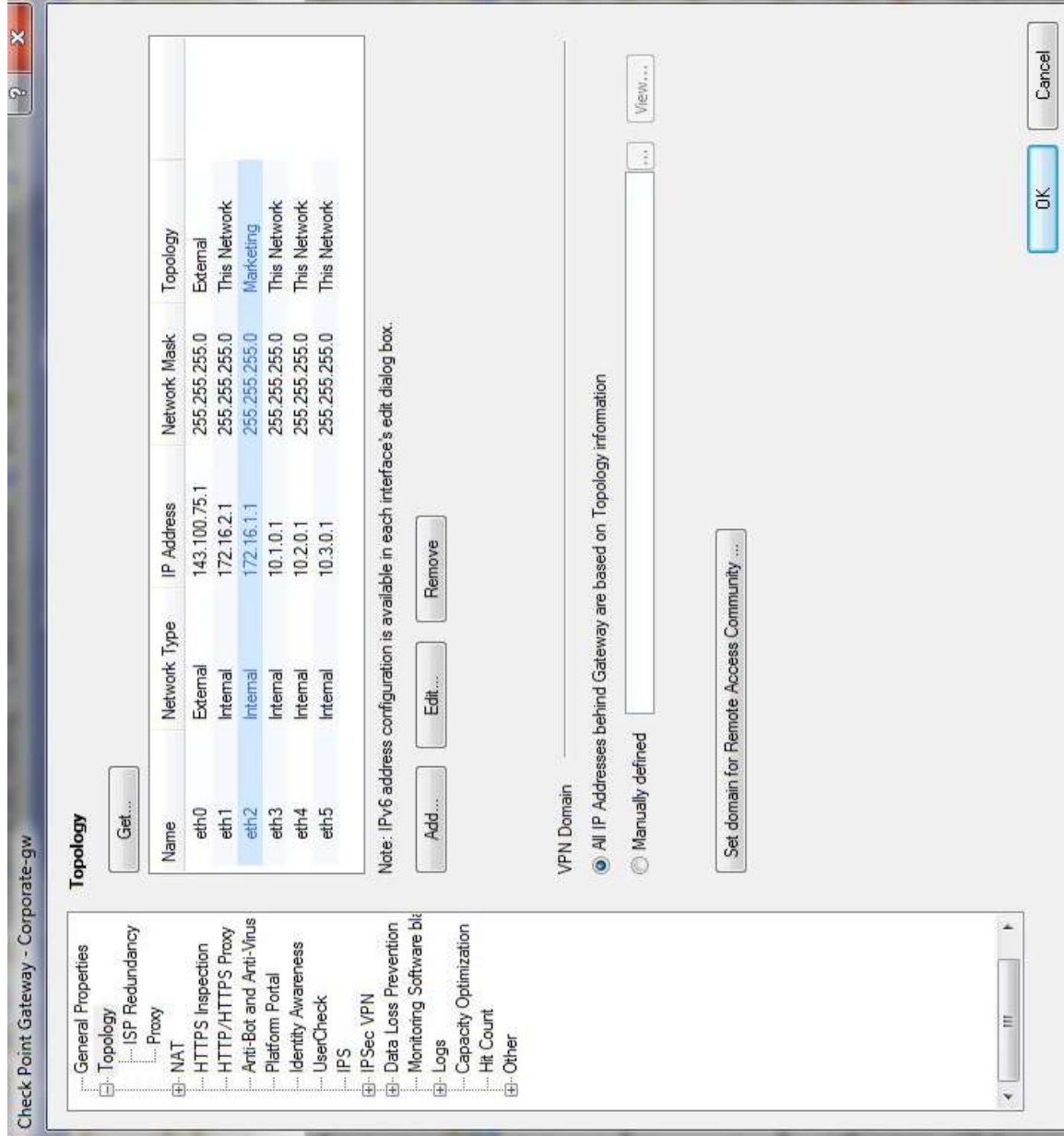
admin

| Network & Endpoint Management | | | | | | | | | | Management | |
|-------------------------------|-----------|----------|-------------------|---------------------|------------------------------|-------------------------|-------------------------|-------------------------|---------|------------------------------------|--|
| Management Queries | | | | | | | | | | Active | |
| Predefined | | | | | | | | | | Records with Session | |
| | | | | | | | | | | All Records | |
| | | | | | | | | | | Custom | |
| No. | Date | Time | Application | Subject | Operation | Object Type | Performed On | Changes | Admin. | General Information | |
| 1 | 27Mar2009 | 10:33:35 | SmartDashboard | User Certificate | Generate User Certificate... | user | David | | fwadmin | | |
| 2 | 27Mar2009 | 10:33:41 | SmartDashboard | Object Manipul... | Create Object | user | David | | fwadmin | | |
| 3 | 27Mar2009 | 10:33:55 | SmartDashboard | Object Manipul... | Modify Object | user | David | Destination: added... | fwadmin | | |
| 4 | 27Mar2009 | 10:35:10 | SmartDashboard | Object Manipul... | Modify Object | firewall_policy | Standard | rule 1 - action: add... | fwadmin | | |
| 5 | 27Mar2009 | 10:36:01 | SmartDashboard | Policy Installation | Install Policy | firewall_application | California_GW | | fwadmin | Security Policy : Standard | |
| 6 | 27Mar2009 | 10:36:40 | SmartDashboard | SIC Certificate | Initialize SIC Certificate | cpshared_application... | California.DMZ.La... | | fwadmin | | |
| 7 | 27Mar2009 | 10:36:44 | SmartDashboard | SIC Certificate | Revoke SIC Certificate | cpshared_application... | California.DMZ.La... | | fwadmin | | |
| 8 | 27Mar2009 | 10:37:27 | SmartDashboard | Policy Installation | Uninstall Policy | firewall_application | California_GW | | fwadmin | | |
| 9 | 27Mar2009 | 10:38:21 | SmartDashboard | Object Manipul... | Modify Object | gateway_ckp | California.DMZ.La... | VPN was removed ... | fwadmin | | |
| 10 | 27Mar2009 | 10:38:21 | SmartDashboard | Object Manipul... | Delete Object | firewall_application | firewall_application... | | fwadmin | | |
| 11 | 27Mar2009 | 10:38:21 | SmartDashboard | Object Manipul... | Delete Object | vpn_application | vpn_application_C... | | fwadmin | | |
| 12 | 27Mar2009 | 10:39:02 | SmartDashboard | Revision Control | Create Version | | Version 2 | | fwadmin | | |
| 13 | 27Mar2009 | 10:39:14 | SmartDashboard | Revision Control | Revert to Version | | Version 2 | | fwadmin | | |
| 14 | 27Mar2009 | 10:39:18 | SmartDashboard | Administrator L... | Log Out | | | | fwadmin | Authentication method: Password | |
| 15 | 27Mar2009 | 10:39:20 | SmartDashboard | Administrator L... | Log In | | | | fwadmin | | |
| 16 | 27Mar2009 | 10:39:29 | SmartView Tra... | Administrator L... | Log Out | | | | fwadmin | | |
| 17 | 27Mar2009 | 10:39:38 | SmartView Tra... | Administrator L... | Log In | | | | fwadmin | Authentication method: Password | |
| 18 | 27Mar2009 | 10:40:21 | User Monitor | Administrator L... | Log In | | | | fwadmin | Authentication method: Password | |
| 19 | 27Mar2009 | 10:40:31 | SmartView Stat... | Administrator L... | Log In | | | | fwadmin | Authentication method: Password | |
| 20 | 27Mar2009 | 10:40:46 | SmartView Stat... | Administrator L... | Force Log Out | | | | fwadmin | Disconnect administrator 'fwadmin | |
| 21 | 27Mar2009 | 10:40:46 | User Monitor | Administrator L... | Log Out | | | | fwadmin | | |
| 22 | 27Mar2009 | 10:41:09 | SmartDashboard | Administrator L... | Log In | | | | fwadmin | Administrator failed to Log in: Wh | |
| 23 | 27Mar2009 | 10:41:11 | SmartDashboard | Administrator L... | Log Out | | | | fwadmin | Administrator failed to Log in: No | |
| 24 | 25Mar2009 | 15:58:22 | System Monitor | Administrator L... | Log In | | | | fwadmin | | |
| 25 | 27Mar2009 | 14:31:22 | SmartView Tra... | Administrator L... | Log Out | | | | fwadmin | connected with user password | |
| 26 | 27Mar2009 | 14:31:36 | SmartView Tra... | Administrator L... | Log In | | | | fwadmin | | |
| 27 | 27Mar2009 | 14:32:24 | SmartDashboard | SIC Certificate | Initialize SIC Certificate | cpshared_application... | Secondary_Manag... | | fwadmin | | |
| 28 | 27Mar2009 | 14:32:24 | SmartDashboard | SIC Certificate | Push SIC Certificate | cpshared_application... | Secondary_Manag... | | fwadmin | | |
| 29 | 27Mar2009 | 14:32:28 | SmartDashboard | Object Manipul... | Create Object | host_ckp | Secondary_Manag... | | fwadmin | | |
| 30 | 27Mar2009 | 14:32:28 | SmartDashboard | Object Manipul... | Create Object | management_appli... | management_appli... | | fwadmin | | |
| 31 | 27Mar2009 | 14:32:28 | SmartDashboard | Object Manipul... | Create Object | cpshared_application... | cpshared_application... | | fwadmin | | |

Antispoofing

Usando a técnica de address spoofing um computador de uma rede externa tenta se passar por uma máquina de uma rede interna modificando o IP de origem de um pacote.

Configuração de Antispoofing



☒ External (leads out to the Internet)
☒ Internal (leads to the local network)
IP Addresses behind this interface:

☐ Not Defined
☐ Network defined by the interface IP and Net Mask
Specific:
☐ Interface leads to DMZ

Anti-Spoofing

☒ Perform Anti-Spoofing based on interface topology
Anti-Spoofing action is set to
☐ Don't check packets from:
Spoof Tracking: ☐ None ☒ Log ☐ Alert

☐ External (leads out to the Internet)
☒ Internal (leads to the local network)
IP Addresses behind this interface:

☐ Not Defined
☐ Network defined by the interface IP and Net Mask
Specific:
☐ Interface leads to DMZ

Anti-Spoofing

☒ Perform Anti-Spoofing based on interface topology
Anti-Spoofing action is set to
☐ Don't check packets from:
Spoof Tracking: ☐ None ☒ Log ☐ Alert