



Holistic **Security** Management



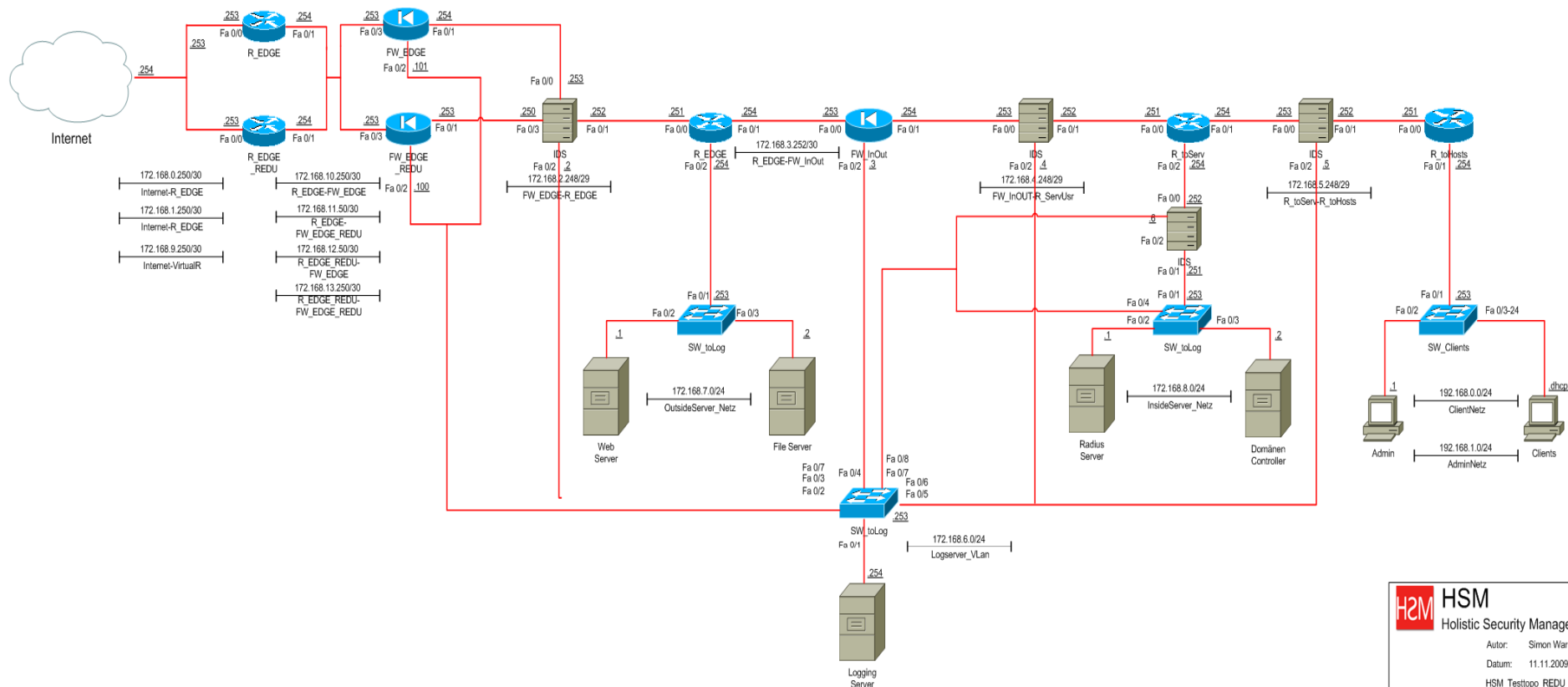
# Holistic **Security** Management

## About

Netzwerksicherheit IT-Recht  
Authentifizierung e-commerce  
Datenschutz Zertifizierung  
ISO 27001  
Hardening IDS Penetration  
Social-Engineering IPS SSL  
Backup Auditing Policy Hacker  
Netzwerksicherheit IT-Recht  
Authentifizierung e-commerce  
Datenschutz Zertifizierung  
ISO 27001  
Hardening IDS Penetration  
Social-Engineering IPS SSL  
Backup Auditing Policy Hacker



# Holistic Security Management Topology





# Holistic Security Management

## Configurations

```
hostname R1_Standort3
service password-encryption
no ip domain-lookup
ip routing
banner modt #Zugriff nur fuer
    autorisierte Administratoren#
ip domain name htl3r.local
crypto key generate rsa
username cisco password cisco
username cisco priv 15
enable secret cisco
line con 0
    logging synchronous
    login local
    exit
line vty 0 1180
    logging synchronous
    login local
    transport input telnet ssh
    exit
line aux 0
    no login
    exit
interface Loopback0
    ip address 172.20.1.6
        255.255.255.248
    exit
interface Loopback1
    ip address 192.168.100.254
        255.255.255.255
    exit
interface Loopback8
    ip address 172.20.1.14
        255.255.255.248
    exit
interface Loopback16
    ip address 172.20.1.22
        255.255.255.248
    exit
interface FastEthernet0/0
    description to_R2_Standort3
    ip address 192.168.10.254
        255.255.255.252
    no shut
    exit
!
interface FastEthernet0/1
    description to_R2_Standort3
    ip address 192.168.10.1
        255.255.255.252
    no shut
    exit
!
interface Serial0/2/0
    description to_R_Standort2
    ip address 10.0.0.254
        255.255.255.252
    no shut
    exit
router ospf 1
    network 172.20.1.0 0.0.0.7 area 1
    network 172.20.1.8 0.0.0.7 area 1
    network 172.20.1.16 0.0.0.7 area 1
    network 192.168.10.0 0.0.0.3 area 1
    network 192.168.10.252 0.0.0.3 area 1
    network 192.168.100.254 0.0.0.0
        area 1
    no auto-summary
    exit
router bgp 65000
    network 172.20.1.0 mask
        255.255.255.248
    network 172.20.1.8 mask
        255.255.255.248
    network 172.20.1.16 mask
        255.255.255.248
    network 192.168.100.254 mask
        255.255.255.255
    neighbor 192.168.30.254 remote-as
        65100
    neighbor 192.168.30.254
```



# Holistic Security Management

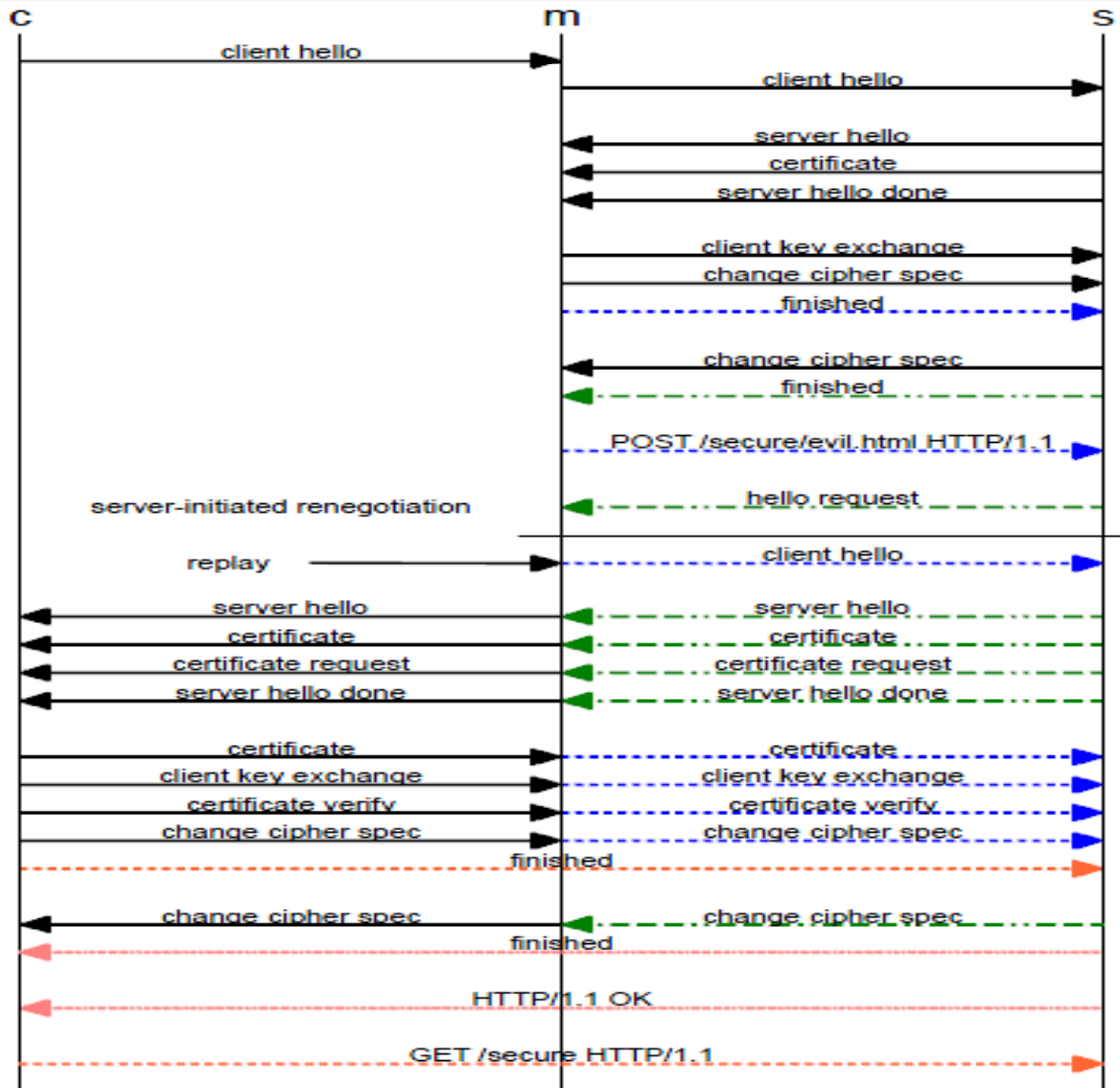
## Log - Files

```
2009-09-10 00:03:41 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:40 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/k
2009-09-10 00:03:41 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:40 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/k
2009-09-10 00:03:41 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:40 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/k
2009-09-10 00:03:41 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/modules/FWResizeFont.js
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114973 for outside:91.141.122.9/1810 to inside:1
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114974 for outside:91.141.122.9/1814 to inside:1
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114975 for outside:91.141.122.9/1812 to inside:1
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114976 for outside:91.141.122.9/1816 to inside:1
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114977 for outside:91.141.122.9/1818 to inside:1
2009-09-10 00:03:41 Local7.Info 10.0.0.42 1833395: 12w2d: %SEC-6-IPACCESSLOGP: list INSIDE_OUT permitted udp 10.2.19.10(51764) -> 10.0.0.100(53), 1 packet
2009-09-10 00:03:41 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/k
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114972 for outside:91.141.122.9/1808 to inside:1
2009-09-10 00:03:41 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/k
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114978 for outside:91.141.122.9/1820 to inside:1
2009-09-10 00:03:41 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/c
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114979 for outside:91.141.122.9/1822 to inside:1
2009-09-10 00:03:41 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114980 for outside:91.141.122.9/1824 to inside:1
2009-09-10 00:03:42 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/images/M_images/pdf_button.png
2009-09-10 00:03:42 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/images/M_images/printButton.pr
2009-09-10 00:03:42 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/images/M_images/emailButton.pr
2009-09-10 00:03:42 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/r
2009-09-10 00:03:42 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/templates/htl3rennweg/images/c
2009-09-10 00:03:42 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114981 for outside:91.141.122.9/1826 to inside:1
2009-09-10 00:03:42 Local4.Info 10.0.0.41 Sep 09 2009 13:48:41 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114982 for outside:91.141.122.9/1828 to inside:1
2009-09-10 00:03:42 Local4.Info 10.0.0.41 Sep 09 2009 13:48:42 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114983 for outside:91.141.122.9/1830 to inside:1
2009-09-10 00:03:42 Local4.Info 10.0.0.41 Sep 09 2009 13:48:42 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114984 for outside:91.141.122.9/1832 to inside:1
2009-09-10 00:03:42 Local4.Info 10.0.0.41 Sep 09 2009 13:48:42 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114985 for outside:91.141.122.9/1834 to inside:1
2009-09-10 00:03:42 Local4.Info 10.0.0.41 Sep 09 2009 13:48:42 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114986 for outside:91.141.122.9/1836 to inside:1
2009-09-10 00:03:43 Local7.Info 10.0.0.42 1833396: 12w2d: %SEC-6-IPACCESSLOGP: list PBR-Policy_von_Administration permitted udp 192.168.21.16(0) -> 192.168.21.31
2009-09-10 00:03:44 Local7.Info 10.0.0.42 1833397: 12w2d: %SEC-6-IPACCESSLOGP: list INSIDE_OUT permitted udp 10.2.9.10(123) -> 192.93.2.20(123), 1 packet
2009-09-10 00:03:46 Local7.Info 10.0.0.42 1833398: 12w2d: %SEC-6-IPACCESSLOGP: list INSIDE_OUT permitted udp 10.2.19.10(51479) -> 10.0.0.100(53), 1 packet
2009-09-10 00:03:51 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:50 ASA-SIL : %ASA-5-304001: 65.55.115.154 Accessed URL 10.0.0.155:/robots.txt
2009-09-10 00:03:51 Local4.Info 10.0.0.41 Sep 09 2009 13:48:50 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114987 for outside:65.55.115.154/35826 to inside
2009-09-10 00:03:51 Local4.Info 10.0.0.41 Sep 09 2009 13:48:51 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114966 for outside:201.51.24.2/4377 to inside:15
2009-09-10 00:03:51 Local7.Info 10.0.0.42 1833399: 12w2d: %SEC-6-IPACCESSLOGP: list INSIDE_OUT permitted udp 10.2.19.10(55076) -> 10.0.0.100(53), 1 packet
2009-09-10 00:03:52 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:51 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/dndocuments/Fototermin_09_10.
2009-09-10 00:03:52 Local4.Info 10.0.0.41 Sep 09 2009 13:48:52 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114988 for outside:91.141.122.9/1838 to inside:1
2009-09-10 00:03:53 Local4.Notice 10.0.0.41 Sep 09 2009 13:48:53 ASA-SIL : %ASA-5-304001: 91.141.122.9 Accessed URL 10.0.0.155:/favicon.ico
2009-09-10 00:03:54 Local4.Info 10.0.0.41 Sep 09 2009 13:48:53 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114989 for outside:91.141.122.9/1840 to inside:1
2009-09-10 00:03:54 Local4.Info 10.0.0.41 Sep 09 2009 13:48:53 ASA-SIL : %ASA-6-106100: access-list ACL_inside_IN permitted udp inside/10.0.0.100(58567) -> outsid
2009-09-10 00:03:54 Local4.Info 10.0.0.41 Sep 09 2009 13:48:53 ASA-SIL : %ASA-6-106100: access-list ACL_inside_IN permitted tcp inside/10.2.9.9(41596) -> outside/
2009-09-10 00:03:54 Local4.Info 10.0.0.41 Sep 09 2009 13:48:53 ASA-SIL : %ASA-6-302016: Teardown UDP connection 12114990 for outside:213.129.232.1/53 to inside:10
2009-09-10 00:03:55 Local4.Info 10.0.0.41 Sep 09 2009 13:48:54 ASA-SIL : %ASA-6-302014: Teardown TCP connection 12114992 for outside:84.112.114.221/63517 to insic
```



# Holistic Security Management

## TLS Handshake





# Holistic Security Management

## RDP Hack

The screenshot shows the main interface of Cain's RDP sniffer. On the left, a tree view lists various protocols under the 'APR' category, including APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-RDP (1), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). The 'APR-RDP (1)' item is selected. The main window displays a table of detected RDP connections:

Started	Closed	RDP server	Client	Status	Cli. Ver.	Et
14/11/2009 - 16:19:19		192.168.0.1	192.168.0.4	Decrypting	RDPv4	m

Below the table, a text editor window titled 'RDP-20091114151919515.txt - Editor' displays the following content:

```
=====  
=== Cain's RDP sniffer generated file ===  
=====
```

[RDP connection]

```
-----  
Server address: 192.168.0.1  
Client address: 192.168.0.4  
-----
```

[Client packet]

```
0000 03 00 01 9c 02 f0 80 7f 65 82 01 90 04 01 01 04 .....e.....  
0010 01 01 01 01 ff 30 19 02 01 22 02 01 02 02 01 00 .....0.....  
0020 02 01 01 02 01 00 02 01 01 02 02 ff ff 02 01 02 .....  
0030 30 19 02 01 01 02 01 01 02 01 01 02 01 01 02 01 0.....  
0040 00 02 01 01 02 02 04 20 02 01 02 30 1c 02 02 ff .....0.....  
0050 ff 02 02 fc 17 02 02 ff ff 02 01 01 02 01 00 02 .....  
0060 01 01 02 02 ff ff 02 01 02 04 82 01 2f 00 05 00 ...../  
0070 14 7c 00 01 81 26 00 08 00 10 00 01 c0 00 44 75 .|...&.....Du  
0080 63 61 81 18 01 c0 d4 00 04 00 08 00 00 04 00 03 ca.....  
0090 01 ca 03 aa 07 04 00 00 28 0a 00 00 4d 00 dc 00 .....(...M...
```

At the bottom of the interface, there are tabs for 'Hosts', 'APR', 'Routing', 'Passwords', and 'VoIP'. The 'APR' tab is active. The status bar at the bottom left indicates 'Lost packets: 0%'.



Holistic **Security** Management  
Contact

<http://www.hsm-pro.at/>

or

Live @  labor